APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/332,358	06/10/1999	ENG-WHATT TOH	3915-US	2834

758   7590   09/25/2003

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA   94041

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/25/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 July 2003</u> .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-28</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-28</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Response to Arguments

1.   This communication is in response to applicants' response received on July 21,

2003.

2.   Applicants' arguments have been fully considered but they are not persuasive.

3.   Applicants on page 2, lines 8-14, argue that: "Applicants' claims generally

concern escrow encryption, where an information package destined for an addressee is

encrypted with an escrow encryption key in response to the addressee not having a

public key. In contrast, in Smith, items are encrypted and an addressee may not

have a public key, but items are NOT encrypted in response to an addressee not having

a public key. Vazana generally does not concern encryption and does not cure the

fundamental shortcomings of Smith. Thus, Applicants respectfully submit that neither

Smith nor Vazana, either alone or in combination, teach or suggest the claimed

invention."

Contrary to applicants argument, with respect to claims 1, 12, 17 and 28, Smith

discloses that the document to be sent to a recipient is encrypted either by the public

key of the recipient or by a secret key (see column 4, lines 50-61). The secret key in

Smith corresponds to the escrow key of the claimed invention. Claim 4 of the examined

application recites that the escrow encryption and decryption keys comprise one of

symmetric keys and asymmetric keys. The symmetric/asymmetric keys are commonly

used in the art for encryption. Thus, escrow encryption process of the claimed invention

is the same as an encryption process using a secret key in Smith.

Smith also discloses that if the recipient does not have a public key, a new pair of

public and private keys are generated (issued) for the recipient (see column 5, lines 5-

29). Then the public key is used to encrypt the secret (escrow) key. The encrypted

secret key is transmitted to the recipient along with the encrypted document (document

is encrypted by the secret key) (see column 5, lines 39-45). During the process of

generating a new pair of public and private keys, the recipient is informed by an e-mail

message (see column 5, lines 7-9) and also the recipient is authenticated (see column

5, lines 19-22). These two actions in Smith correspond to the recited "notifying the

addressee..." and "...acknowledgment from the addressee". Also during the process of

generating the public key for the recipient, the document either kept at the sender

computer (see column 5, lines 32-36) or transmitted to the delivery server via a secure

channel (see column 5, lines 60-62). In either case the document is secured which

corresponds to the recited "storing the package in escrow for the addressee".

Vazana teaches a system that stores messages (data or document) for a

recipient in a host computer and informs the recipient of the stored (escrowed)

messages (see column 3, lines 14-24 and column 5, line 52-column 6, line 3). However,

examiner contends that at the time the invention was made, a person of ordinary skill in

the art would be motivated to implement the storage of a transmitting document in the

delivery server of Smith as taught in Vazana, because it would provide for storing the

document in a secure place until it is transmitted to the intended recipient upon

receiving the recipient public key.

4.   However, In light of the above submission examiner maintains the previous claim

rejections 35 USC § 103.

5.   **Previous Rejection**

Claim Rejections - 35 USC § 103

.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

1.   Claims 1-28 are rejected under 35 USC 103(a) as being unpatentable over Smith

et al (6,061,448) (hereinafter Smith) in view of Vazana (5,850,519).

.   Claims 1-3, 5, 12-14 and 28

Smith discloses a system for secure document delivery over an open network,

such as Internet (col. 4, lines 26-61). The document is sent from a sender to a recipient

via a delivery sever. In this system, upon the sender's direction the delivery server

determines whether the recipient has a public key by querying a database (directory) (col. 4, lines 37-49 and col. 6, lines 11-15). In the event that the recipient does not have a public key (co. 5, lines 5-15) the server sends an e-mail message (a notification) to the recipient containing a dynamically generated URL. Recipient dynamically downloads a Java Applet or Plug-in by accessing the URL. This Applet or Plug-in then runs on the recipient system and generates a private/public key pair. The new public key is sent (col. 5, lines 15-29) to the delivery server and from there to the certificate authority for storage (a public key directory). The delivery server may simply keep the public key in a local database. The delivery sever authenticates the recipient by using the recipient e-mail address and the properties of the generated URL. After the authentication the server transmits the recipient's public key to the sender. The sender uses the recipient's public key (col. 5, lines 30-45) to encrypt a secret key (corresponding to the recited escrow key) that has been used for encryption of the document to be delivered to the recipient. Afterward, the sender transmits the encrypted document, the recipient's address and the encrypted secret key to the delivery server to be delivered to the recipient. In another embodiment of the Smith system (col. 5, lines 60-65) the delivery server encrypts the document received from the sender using a secret key corresponding to the recited escrow key and encrypts the secret key using the recipient's public key. The server then sends the encrypted document and the encrypted secret key to the recipient. In yet another embodiment, the server of the Smith system (col. 6, lines 3-10) may use the recipient's public key to encrypt the document. The encrypted document is then transmitted to the recipient.

Computer programs such as the Send Client within the sender computer, the

Delivery Server software within the server computer and the Receive Client within the

recipient computer are adapted to accomplish the above functions (col. 8, lines 1-18).

Smith does not disclose expressly the storing of the encrypted document to be

delivered to the recipient on the delivery server in neither cases that the recipient is

having a public key or not.

Vazana discloses a system of delivering electronic messages (abstract) from a

sender to a recipient in which the message is stored in the mailbox of the recipient on at

least one main host computer (a server) (col. 3, lines 14-24.) The host computer (col. 5,

line 52-col. 6, line 3) after storing the message in the intended recipient's mailbox,

contacts the recipient via a dialing unit to notify the recipient of the stored message

awaiting collection.

Smith and Vazana are analogous art because they are from the same field of

endeavor that is delivering information from a sender to a recipient over an open

network using at least one server in between.

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to include an storage area in the delivery server of Smith as

thought in Vazana because it would provide for storing (in escrow) the electronic

information on the server (Vazana, col. 2, lines 29-34 and col. 3, lines 25-30) to be

retrieved by the intended recipient upon receiving notification from the server.

Claims 4 and 7

Claims 4 and 7 are rejected over Smith in view of Vazana as applied to like

elements of Claims 1-3 above and the following.

Smith (col. 4, lines 50-56) provides a secret key corresponding to the recited

escrow key, for encryption and decryption of a document (col. 3, lines 64-67) to be

transferred to a recipient. Smith also teaches that any encryption scheme (symmetric or

asymmetric) (col. 4, lines 57-67) known in the art can be utilized for the secure

transmission of information between a sender and a recipient.

Claim 6

Claim 6 is rejected over Smith in view of Vazana as applied to like elements of

Claims 1-3 above and the following.

Smith (col. 5, lines 5-15) teaches that the delivery server notifies recipient via e-

mail that there is no recipient's public key in the public key database.

Claim 8

Claim 8 is rejected over Smith in view of Vazana as applied to like elements of

Claims 1-3 above and the following.

Smith (col. 5, lines 5-15) teaches that the secret key corresponding to the recited

escrow key is not the same as the public and private keys of the recipient.

Claim 9

Claim 9 is rejected over Smith in view of Vazana as applied to like elements of

Claims 1-3 above and the following.

Smith (col. 5, lines 17-25) teaches that the server authenticates the recipient

using the recipient's e-mail address after receiving the public key of the recipient via e-

mail that includes the recipient's name and e-mail address.

Claim 10, 11 and 15

Smith discloses that the delivery server upon the sender's request, queries a

database to retrieve the recipient's public key (col. 4, lines 39-41). The sender uses the

retrieved public key to encrypt the document (col. 3, lines 14-19). The encrypted

document is then transmitted to the recipient via a network and only an intended

recipient is permitted (an authenticated user) to gain access to the encrypted document

(col. 3, lines 52-63).

However, Smith does not disclose expressly the storing of the encrypted

document and notifying the intended recipient of the stored document.

Vazana discloses a system of electronic mail transmission in which the message

is stored on the server and the recipient is notified of the awaiting message for

collection (col. 6, lines 50-54).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to store the encrypted document on the delivery server of Smith as thought in Vazana because it would provide for the encrypted document to await the recipient until the recipient retrieves the document (Vazana, col. 2, lines 29-34 and col. 3, lines 25-30). This would especially be advantageous when the recipient is immediately not available (Vazana, col. 6, lines 56-59).

Claim 16

This claim is rejected over Smith in view of Vazana as applied to like elements of claims 1-3 above and the following.

Smith discloses (col. 3, lines 14-18) that the document is encrypted using the recipient public key. The encrypted document is then transmitted to the recipient and decrypted using the new private key associated with the public key.

Claims 17 and 23

Smith discloses the use of:

A programmatic interface corresponding to the recited directory interface, to access a database in determining whether the recipient has a public key (col. 6, lines 46-55);

A secret key corresponding to the recited escrow key for encryption of the document to be transferred to the recipient (col. 4, lines 50-55);

A Send Client (a software module) (col. 6, lines 9-10) to be used by the sender to encrypt the secret key and the document to be delivered to the recipient (col. 5, lines 30-45);

A computer code (corresponding to the recited notification module) that is used by the delivery server (col. 5, lines 5-11 and col. 8, lines 1-7) to send messages to the recipients via a network;

A computer module (col. 5, lines 10-15), such as an applet or plug-in to generate public and private keys for the recipient in response to the notification from the delivery server; and

A computer code (by the delivery server) (col. 7, lines 46-51 and col. 7, lines 30-35) for transmission of the encrypted document to the recipient(s).

Smith, however, does not disclose expressly the use of a storage area on the delivery server to store the encrypted document to be delivered to the recipient.

Vazana discloses the use of a storage area on the main host computer (the server) (col. 3, lines 19-24 and Fig. 2, item 70) to store (in escrow) the electronic mail for the addressee.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include an storage area in the delivery server of Smith as thought in Vazana because it would provide for storing (in escrow) the electronic information on the server (Vazana col. 2, lines 29-34 and col. 3, lines 25-30) to be retrieved by the intended recipient upon receiving notification from the server.

Claim 18

This claim is rejected over Smith in view of Vazana as applied to like elements of claim 17 above and the following.

Smith discloses the storing of the recipient's public key (col. 5, lines 25-29 and col. 6, lines 50-67) in a database that either is residing on the delivery server or on a separate server.

Claim 19

This claim is rejected over Smith in view of Vazana as applied to like elements of claim 17 above and the following.

Smith discloses that the software module (applet or plug-in), after generating the public and private keys (col. 5, lines 16-29), transmits the recipient public key to the delivery server to be stored in a database for future use.

Claim 20

This claim is rejected over Smith in view of Vazana as applied to like elements of claim 17 above and the following.

Smith discloses that the delivery sever (col. 5, lines 5-11) uses a software to notify the recipient by e-mail message that there is no public key for the recipient in the database.

Claim 21

This claim is rejected over Smith in view of Vazana as applied to like elements of
claim 17 above and the following.

Smith discloses that the secret key corresponding to the recited escrow key is
provided to the users (col. 1, lines 33-55 and col. 7, lines 52-62) via a secure channel to
be used as encryption and decryption key by the users.

Claim 22

This claim is rejected over Smith in view of Vazana as applied to like elements of
claims 4 and 17 above.

Claims 24 and 25

These claims are rejected over Smith in view of Vazana as applied to like
elements of claim 17 and 23 above and the following.

Smith discloses (col. 5, lines 5-15) that the Java Applet or Plug-in (corresponding
to the recited registration module) that generates the recipient's public and private keys
is transmitted to the recipient by the delivery server in an e-mail message (attachment).
The recipient receives the said module by accessing a URL link (hyperlink).

Claim 26

This claim is rejected over Smith in view of Vazana as applied to like elements of
claim 17 and 23 above and the following.

Smith discloses (col. 7, lines 31-60 and col. 8, lines 1-10) that the delivery server is configured to forward to the recipient the secret key corresponding to the recited escrow key and the encrypted document. The Receive Client (a software) of the recipient receives the document and the secret key and uses the secret key to decrypt the document.

Claim 27

This claim is rejected over Smith in view of Vazana as applied to like elements of claim 17 and 23 above and the following.

Smith discloses (col. 7, lines 26-30) that the Send Client (a software) of the sender transmits to the delivery server the encrypted secret key corresponding to the recited escrow key and the encrypted document. The delivery server may decrypt the document using the secret key and alternatively re-encrypt the document (col. 6, lines 3-5) by using the recipient's public key. The encrypted document is then sent to the recipient. The Receive Client within the recipient receives the encrypted document (col. 7, lines 35-40) and uses the recipient private key to decrypt the document.

Conclusion

3.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
September 16, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100